UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,154	11/24/1999	PAUL S. GERMSCHEID	33012/274/10	4721

7590 07/02/2003

CHARLES A JOHNSON
UNISYS CORPORATION
LAW DEPARTMENT M S 4773
2470 HIGHCREST ROAD
ROSEVILLE, MN 55113

EXAMINER
WASSUM, LUKE S

ART UNIT	PAPER NUMBER
2177	9

DATE MAILED: 07/02/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/448,154	GERMSCHEID ET AL.	
	Examiner	Art Unit	
	Luke S. Wassum	2177	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 April 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Response to Amendment

1. The Applicants' amendment, filed 31 March 2003, has been received, entered into the record, and considered.

2. As a result of the amendment, claims 1, 6, 11 and 16 have been amended. Claims 1-20 remain pending in the application.

Specification

3. The disclosure is objected to because of the following informalities:

On the replacement page 33, submitted as part of Amendment A, at line 23, there is a typographical error. The cited patent application number, 09/188549, should be 09/188649.

Additionally, there seems to be inconsistencies between different sections of the specification. In the Summary of the Invention, pages 7-9, a site-specific security profile is discussed, such that there is no need to transmit UserID/password information across a publicly accessible network. However, in connection with Figure 10, replacement pages 33-34, the Detailed Description of the Preferred Embodiments discusses the user's service request resulting in the execution of a command language script with associated security profile which requires the user to submit a UserID over the World Wide Web in order for the execution of the script to proceed. The examiner has failed to locate a disclosure of site-specific security profile anywhere in the Detailed Description of the Preferred Embodiments.

4. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code, for instance, at page 27, line 21, and at page 28, line 2. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

6. Claims 1-20 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The claim limitations of the independent claims regarding the use of a physical site specific security profile in permitting access to a database without requiring the transfer of a user identifier via a publicly accessible digital data communications network (claims 1, 6, 11 and 16) are discussed in the Summary of the Invention, pages 7-9. However, the details of the use of the physical site specific security profile is not disclosed in the Detailed Description of the Preferred Embodiments, and in fact the section of the Detailed Description concerning the operation of security profiles discloses a mechanism whereby a user submits a service request which results in the execution of a

command language script with associated security profile which requires the user to submit a UserID over the World Wide Web in order for the execution of the script to proceed. This disclosure is inconsistent with the claim language. The lack of a detailed disclosure of the claimed invention renders the invention non-enabled.

Claims 2-5, 7-10, 12-15 and 17-20 are also rejected as being non-enabled, inheriting the deficiencies of their parent independent claims, and furthermore because other claimed details, such as the "special field" of claims 3, 7, 13 and 17, and the mechanism for the generation of the physical site specific security profile by the database management system (claims 3 and 6), are not disclosed in the specification.

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The claim language, as discussed above with regard to 35 U.S.C. 112 first paragraph, is inconsistent with the disclosure of the invention. This inconsistency renders the claims indefinite, in accordance with MPEP § 2173.03[R-1]:

> "Although the terms of a claim may appear to be definite, inconsistency with the specification disclosure or prior art teachings may make an otherwise definite claim take on an unreasonable degree of uncertainty. In re Cohn, 438 F.2d 989, 169 USPQ 95 (CCPA 1971); In re Hammack, 427 F.2d 1378, 166 USPQ 204 (CCPA 1970). In Cohn, the claim was directed to a process of treating a surface with a corroding solution until the metallic appearance is supplanted by an "opaque" appearance. Noting that no claim may be read apart from and independent of the supporting disclosure on which it is based, the court found that the description, definitions and

> examples set forth in the specification relating to the appearance of the surface after treatment were inherently inconsistent and rendered the claim indefinite."

The Invention

9. The instant invention is a data processing system containing site-specific security profiles, such that the user is allowed to access a database only from a specific terminal or location.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 1-4, 6-8, 11-14 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems").

13. Regarding claim 1, **Garrison** teaches a data processing environment having a user terminal at a site for generating a service request responsively coupled via a publicly accessible digital data communication network to a database management system having at least one database as claimed, comprising security profile corresponding to a site whereby said database management system permits said user terminal to access said at least one database (see col. 4, lines 1-32; see also col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a data processing environment wherein the security profile is site-specific.

Yoshimoto, however, teaches a data processing environment wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches a data processing environment wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

14. Regarding claim 6, **Garrison** teaches an apparatus as claimed, comprising:

a) a user terminal located at a site (see col. 4, lines 1-32);

b) a database management system having access to a database responsively coupled to said user terminal via a publicly accessible digital data communication network (see col. 4, lines 1-32); and

c) a security profile generated by said database management system corresponding to said site whereby said database management system provides access to a particular portion of said database corresponding to said security profile (see col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach an apparatus wherein the security profile is site-specific.

Yoshimoto, however, teaches an apparatus wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

15. Regarding claim 11, **Garrison** teaches a method of utilizing a user terminal located at a site to access a remote database management system having a database via a publicly accessible digital data communication network as claimed, comprising:

a) transmitting a service request requiring access to said database from said user terminal (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

b) receiving said service request by said remote database management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

c) determining a security profile corresponding to said site (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37);

d) comparing said security profile with said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and

e) honoring said service request if and only if said service request corresponds to said security profile (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach a method wherein the security profile is site-specific.

Yoshimoto, however, teaches a method wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches a method wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

16. Regarding claim 16, **Garrison** teaches an apparatus as claimed, comprising:

a) means located at a site for permitting a user to interact with a database responsively coupled via a publicly accessible digital data communication network (see col. 4, lines 1-32);

b) means responsively coupled to said permitting means via said publicly accessible digital data communication network for offering data processing services involving access to

said database in response to said service request (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37); and

c) means responsively coupled to said offering means for preventing said offering means from offering said data processing services to said user in response to said service request unless said site corresponds to a security profile wherein said security profile permits access to said database (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

Garrison does not explicitly teach an apparatus wherein the security profile is site-specific.

Yoshimoto, however, teaches an apparatus wherein the security profile is site-specific (see Abstract; see also col. 1, line 63 through col. 2, line 6).

It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate a site-specific security profile, since this would allow the level of access granted to a user to be based in part on the security of the specific terminal or location from which the access request is generated, thus inhibiting illegitimate access from a terminal having poor security (see **Yoshimoto**, col. 6, lines 15-21).

Neither **Garrison** nor **Yoshimoto** explicitly teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network.

De Capitani di Vimercati et al., however, teaches an apparatus wherein the user accesses the database without transfer of said user identifier via said publicly accessible digital data communication network (see page 88, col. 2, last paragraph; see also Table 1; see also section 3.2 Authentication, beginning on page 94, all of which teach a mechanism whereby all users accessing a database from a particular site are granted access).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the three references, since they are all concerned with the same field of endeavor, that is, remotely accessing databases (see **Garrison**, Abstract; see also **Yoshimoto**, Abstract; see also **De Capitani di Vimercati et al.**, Abstract).

It would have been furthermore obvious to one of ordinary skill in the art at the time of the invention to provide an authentication mechanism whereby the user identifier need not be transmitted via a publicly accessible digital communication network, since it is necessary to protect all information transferred over the global communication network (see **Capitani di Vimercati et al.**, page 93, col. 2, second to last paragraph).

17. Regarding claim 2, **Garrison** additionally teaches an improvement wherein said security profile is generated by said data management system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

18. Regarding claims 3, 8, 12, 13 and 18, **Garrison** additionally teaches an improvement, method and apparatus further comprising a special field responsively coupled to a service request whereby said database management system receives said special field and generates said security profile

corresponding to said site and to said special field (see discussion of predefined password at col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

19. Regarding claims 4, 14 and 17, **Garrison** additionally teaches an improvement, method and apparatus wherein said publicly accessible digital data communication network further comprises the Internet (see col. 4, lines 1-32).

20. Regarding claim 7, **Garrison** additionally teaches an apparatus wherein said user terminal accesses said data entity by transferring a service request to said system (see col. 6, line 60 through col. 7, line 32; see also col. 7, line 50 through col. 8, line 37).

21. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **King** ("Hazards Control Department Use of the Sperry Database Management System MAPPER").

22. Regarding claims 5, 9, 15 and 19, **Garrison, Yoshimoto** and **De Capitani di Vimercati et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, Yoshimoto** nor **De Capitani di Vimercati et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **King** teaches a system wherein the database management system used is MAPPER (see first paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER is extremely versatile and is considered one of the best fourth generation programs, and furthermore since it contains, in addition to a database management system, a word processor, office automation program including electronic mail, and color graphics routines (see **King**, first paragraph).

23. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

24. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

25. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Unisys** ("Why Do I Need Cool ICE?").

26. Regarding claims 5, 9, 15 and 19, **Garrison, Yoshimoto** and **De Capitani di Vimercati et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, Yoshimoto** nor **De Capitani di Vimercati et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Unisys** teaches a system wherein the database management system used is MAPPER (see page 3, second paragraph).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER has been tuned for reliability, scalability, and high performance, and furthermore, since the technology has been used for years by thousands of users for many different kinds of applications, and since it has gained a reputation for performing well for everything from small data analysis applications to huge transaction systems, and since its reliability is exemplary (see **Unisys**, page 3, second paragraph).

27. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

28. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

29. Claims 5, 9, 10, 15, 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Garrison** (U.S. Patent 6,275,939) in view of **Yoshimoto** (U.S. Patent 6,237,023) in view of **De Capitani di Vimercati et al.** ("Access Control in Federated Systems") as applied to claims 1-4, 6-8, 11-14 and 16-18 above, and further in view of **Gebauer** (U.S. Patent 6,324,539).

30. Regarding claims 5, 9, 15 and 19, **Garrison, Yoshimoto** and **De Capitani di Vimercati et al.** teach an improvement to a data processing environment, method and apparatus substantially as claimed.

None of **Garrison, Yoshimoto** nor **De Capitani di Vimercati et al.** explicitly teaches the improvement, method and apparatus wherein said database management system is MAPPER.

However, **Gebauer** teaches a system wherein the database management system used is MAPPER (see col. 1, lines 56-65).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use MAPPER as the database management system, since MAPPER is one of the most successful database management systems available (see **Gebauer**, col. 1, lines 56-65), and furthermore that providing access to a proprietary database management system such as MAPPER through the Internet would yield an extremely inexpensive and universally available means for accessing the data which it contains and such access would be without the need for considerable specialized training (see **Gebauer**, col. 2, lines 45-51).

31. Regarding claim 10, **Garrison** additionally teaches an apparatus wherein said publicly accessible digital data communication network further comprises the World Wide Web (see col. 4, lines 1-32).

32. Regarding claim 20, **Garrison** additionally teaches an apparatus wherein said permitting means further comprises an industry standard personal computer (see col. 4, lines 1-60).

Response to Arguments

33. Applicant's arguments filed 31 March 2003 have been fully considered but they are not persuasive.

34. Regarding the Applicants' argument that the **Yoshimoto** reference would not have been compatible with that of **Garrison**, the examiner respectfully responds that the **Yoshimoto** reference cites the fact that the disclosed network includes a WAN constructed by interconnected networks (see col. 3, lines 42-47). The Internet is an example of just such a network. Furthermore, the reference also cites the use of a TCP/IP protocol (see col. 4, lines 18-23), the same protocol that is used on the Internet.

35. Regarding the Applicants' argument that there is no showing of a reasonable expectation of success, the examiner respectfully replies that the fact that the combined references are concerned with the same field of endeavor, that is, the access of remote databases, and that the secondary

references are relied upon merely for different security features, ensures that there would have been a reasonable expectation of success in combining the references as cited.

Conclusion

36. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gebauer et al. (U.S. Patent 6,496,821) teaches a method of profiling columns on the basis of the security profiles of specific groups in a Cool ICE system.

37. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luke S. Wassum whose telephone number is 703-305-5706. The examiner can normally be reached on Monday-Friday 8:30-5:30, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on 703-305-9790. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

In addition, INFORMAL or DRAFT communications may be faxed directly to the examiner at 703-746-5658.

Customer Service for Tech Center 2100 can be reached during regular business hours at (703) 306-5631, or fax (703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Luke S. Wassum
Art Unit 2177

lsw
June 26, 2003

JEAN R. HOMERE
PRIMARY EXAMINER